Tips for evaluating, planning, preparing, and piloting a Microsoft Windows 2000 environment

integration note, 2nd Edition

Abstract

This integration note provides tips on evaluating, planning, preparing, and piloting a Microsoft 2000 environment.

It includes an evaluation of Windows 2000, presents a benefit and cost analysis, and then lets you decide if this revolutionary operating system is right for you.

Next are tips on how to plan and prepare for upgrading to Windows 2000, including Active Directory design considerations, some of which are based on HP's own criteria.

After these design tips are suggestions on piloting and validating a Windows 2000 environment—including the selection of a particular upgrade strategy—and explanations of how to get help in designing and piloting your own Windows 2000 environment.

Most importantly, when you decide to use Windows 2000, there are suggestions that allow you to immediately start the planning and preparation phases. Although this might take a few months, you will be miles ahead of the competition and can more quickly reap the benefits when you install Windows 2000.

For more information on Microsoft Windows 2000, check out the following white papers: *Implementing Microsoft Windows 2000 with Service Pack 4 on ProLiant servers* and *Upgrading to Microsoft Windows 2000 on ProLiant servers*, which are located on the ISS Technology Papers website at www.hp.com/servers/technology.

Your strategy should include checking the HP Windows 2000 website at http://h71028.www7.hp.com/enterprise/cache/8181-0-0-0-121.aspx for new information on a regular basis. The HP Services website at www.hp.com/hps/ can help you plan your upgrade to Windows 2000.

Other sources of information include the HP Frontline Partnership site at www.hp.com/go/microsoft.

Symbols in text

The following symbols can be found in the text of this document:

⚠ **WARNING:** Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

△ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

✓ **IMPORTANT:** Text set off in this manner presents clarifying information or specific instructions.

📝 **NOTE:** Text set off in this manner presents commentary, sidelights, or interesting points of information.

Overview

On October 27, 1998, Microsoft announced new packaging and licensing for its developing Windows NT 5.0 and officially renamed this revolutionary OS platform as Microsoft Windows 2000.

Windows 2000 is not simply an incremental upgrade but a radical new design. The preparation time for designing and implementing this powerful new OS could take as long as 4 to 6 months. Starting

with small pilots will allow a better understanding of how and if Windows 2000 will work in your environment.

Some concerned customers have asked:

- Is Windows 2000 worth the effort?
- When will I see a return on my investment?
- How do I begin planning for Windows 2000?
- How do I prepare my current Windows NT system for Windows 2000?
- What's the Active Directory and how do I design one for my company?
- Can anybody out there help me?"

HP system architects, engineers, and technicians can help you. HP has been working with Microsoft on this project since March 1996 when Microsoft invited the Information Management team to join its newly initiated Deployment Program for Windows 2000. The program's objective was to create awareness and gain practical feedback from customers on the deployment of Windows 2000 before actual release. Working hand in hand, HP and Microsoft have designed, tested, and challenged the boundaries of Windows 2000. The majority of Windows 2000 code has been developed on HP products; all Deployment Program events run on HP equipment; and Microsoft test labs continue to use HP hardware.

Both companies are now ready to share their knowledge and experience to help you reduce the learning curve and more efficiently design and pilot your own Windows 2000 environment.

Start with this Integration Note. It provides some helpful tips to get you started, and will, hopefully, answer some of your questions and concerns about Windows 2000 and its deployment. More specifically, it offers guidance and tips in the following areas:

- Evaluating Windows 2000
- Planning and preparing for Windows 2000
- Understanding and designing Active Directory
- Piloting your Windows 2000 environment
- Developing an upgrade strategy
- Getting additional information and support

Evaluating Windows 2000 products

The Windows 2000 Professional (workstation) and the Windows 2000 Server family—Server, Advanced Server, and Datacenter Editions work together to enhance the management of Windows networks.

Windows 2000 Professional (Workstation)

Windows 2000 Professional combines the strengths of Windows NT Workstation 4.0 with the best business features of the Windows 98 operating system. It also supports upgrades from Windows 95, Windows 98, and Windows NT Workstation 4.0.

Windows 2000 Professional makes users more productive and lowers the total cost of ownership (TCO) by using a simpler, more intelligent interface than that of Windows NT 4.0. This interface includes personalized menus that streamline the familiar Windows interface and reduce clutter by removing less used desktop items. A built-in algorithm continually monitors program use, shortcuts, and the files that users access from the start menu, and then arranges the menu for easy access to the most commonly used options. In addition, new wizards help administrators simplify workstation configurations and settings.

Using Windows 2000 on the client side automates common web tasks for purposes of intranet communications. For example, AutoComplete finishes incomplete web addresses, and AutoCorrect fixes simple typing errors. In addition, technology from IntelliForms recalls web-form data, such as names and addresses, and intelligent network-setting detection makes accessing the Internet easier, even when moving users from LAN to dial-up connections. Evidence of these features may already be seen in Internet Explorer 5.0 or Microsoft Office 2000.

Windows 2000 Server Edition

Microsoft 2000 Server, which replaces Microsoft Windows NT Server, delivers higher levels of overall system reliability and scalability than its predecessor. To help lower costs, Windows 2000 Server delivers comprehensive management services for servers, networks, and Windows-based client systems.

Windows 2000 Server also extends the application services established by Windows NT Server 4.0. By integrating application services such as COM+, transaction and message queuing, and XML support, Windows 2000 Server is an ideal platform for turnkey Independent Software Vendor (ISV) solutions, as well as custom, line-of-business applications.

Reflecting the continuing rapid progress in microprocessor speeds, Windows 2000 Server supports uniprocessor systems and 4-way symmetric multiprocessing (SMP) systems with up to 4 GB of physical memory. Many HP ProLiant servers are ideal for this OS platform.

At the core of Windows 2000 Server is a complete set of infrastructure services based on the Active Directory services. The Active Directory provides a centralized way to manage users, groups, and network resources; strengthens security; and extends interoperability with a variety of applications and devices.

Organizations increasingly rely on advanced web technologies to more effectively communicate with partners and employees, and Windows 2000 Server delivers. From simple site hosting to advanced web applications and streaming media services, Windows 2000 Server provides an integrated flexible web platform with the full range of services organizations need to deploy intranets and critical web-based business solutions.

Windows 2000 Server is best sized for small- to medium-sized application deployments, web servers, and organizations with numerous workgroups and branch offices.

Windows 2000 Advanced Server

Replacing the Windows NT Server 4.0 Enterprise Edition, Windows 2000 Advanced Server is a more powerful server operating system. It provides all the benefits of the Server Edition and integrates high-availability clustering, network, and component load balancing to provide excellent system and application availability for demanding enterprise operations.

Ideal for database-intensive work, Advanced Server supports systems with 8 GB of memory and up to 8-way SMP.

Windows 2000 Datacenter Server Edition

Windows 2000 Datacenter Server is a specialized high-end version of Windows 2000 Server, supporting up to 32-way SMP and up to 64 GB of physical memory. Like Windows 2000 Advanced Server, it provides clustering and load balancing services as standard features; however, it provides a more advanced 4-node clustering. In addition, Windows 2000 Datacenter is optimal for large warehousing, econometric analysis, large-scale simulations in science and engineering, online transaction processing, server consolidation, and large-scale ISPs and website hosting.

The Server Edition is the most popular version for small- to medium-sized businesses. The Advanced Server and Datacenter Editions are designed to meet the needs of mission-critical deployments in

medium to large enterprises and Internet Service Provider (ISP) organizations. In fact, Windows Advanced Server and Windows 2000 Datacenter systems are designed to support more than 10,000 simultaneous users in some workloads, while continuing to provide record-setting price performance in transaction processing.

Summary of Windows 2000 features and their benefits

Windows 2000 provides many new features, functionality, and benefits:

- Active Directory, a key enhancement to Windows 2000 over previous versions of Windows NT, that offers enterprise-wide user management
- You will be able to consolidate your domains and simplify your infrastructure management since Active Directory eliminates the artificial limitations of Windows NT domains.
- You will have one place to store all user information, which means you do not have to worry about duplicate usernames anymore. You will have only one place to look for objects and only one place to manage. As a result, you do not have to spread yourself thin over many domains and many servers.
- For the first time you will have the opportunity to require certain behaviors on the network. For example, HP has an internal policy that requires all users—whether they are logging on inside the company or dialing in remotely—to be running real-time virus-scanning software. Under Windows NT 4.0 there is no way to enforce this kind of policy. With Windows 2000, you can enforce it.
- You will have better control over the client machine and it will be easier to administer. For example, monthly CDs will keep your clients completely up to date with the rest of the network, and they will still be able to do their dialing for mail.
- You will be able to delegate domain management functions in ways that make sense for your organization, rather than by proximity to domain controllers. See the section "Understanding the Structure and Function of Active Directory."
- Better hardware support (faster performance and greater reliability, as well as protected information) and most manageable environment (with the lowest TOC)
- Improved user interface (richer functionality)
- A more standards-based environment that enables large enterprise-class companies to purchase mainstream off-the-shelf software and reduce the cost of operations and complexity
- Features not available in Windows NT 4.0 and provided through ProLiant value-added software now an inherent part of Windows 2000: PC Card support and Advanced Configuration and Power Interface (ACPI)
- Enhanced security features of Kerberos, public key integration, and Bio-metric validation
- Comprehensive Internet and applications support

Primary cost elements

The major cost of Windows 2000 stems from the fact that this operating system is more revolutionary than evolutionary. This creates a learning curve that requires training, as well as planning and piloting a Windows 2000 environment. The HP Information Management team spent a solid six months working out the best way to implement Windows 2000. You might have to spend the time and the effort to do the same because there is really a large change in the way Windows 2000 works. However HP has been involved from the start and can guide you through the process. See the section "HP Support for Windows 2000."

NOTE: Do not forget those applications that will require additional memory.

Another major cost is equipment. To run Windows 2000, Microsoft recommends minimums of Pentium 166, 32 MB of RAM, and 2 GB of hard disk space for workstations; and 300-MHz Pentium II with 128 MB of RAM and 2 GB of hard disk space for servers.

To gain the full benefits of Windows 2000—in particular the capability to place millions of objects under one domain—you might consider upgrading to newer, more robust HP servers.

Return on investment (ROI)

Due to the costs described in the last section, do not be disappointed if you do not see a ROI in the first year. However, after implementation, you will immediately begin seeing rewards in two major areas:

- A drastic reduction in the amount of handholding you do with your users. If your user has a problem today, it almost always requires that a technician go to the client machine and analyze the situation. That means that at least two people are unproductive for however long the problem takes to fix. Once you go to Windows 2000, 95 percent of user problems could probably be solved remotely from a central location by just one qualified technician.
- A huge reduction in network administrators at remote locations. Because Windows 2000 is so remotable, you no longer need 7 x 24 support at every location. Support could come from anywhere in the world. At HP, for example, we required two 12-hour work shifts—at each location––to support our operations; with Windows 2000, we can rely on remote support locations (which are in the daytime cycle) to support other operations that are in their nighttime cycle.
- A drastic reduction in the number of machines needed to manage your infrastructure. The reduction in the number of machine that you have to manage, upgrade, and monitor will create a huge benefit in operating costs.

Planning and preparing a Windows 2000 environment

Here are some basic steps to get you started planning for your Windows 2000 upgrade:

1. Establish functional teams.
2. Understand the structure and function of Active Directory.
3. Examine your current system.
4. Prepare your current system for Windows 2000.
5. Pilot and validate your Windows 2000 environment.
6. Explore upgrade strategies: restructuring and migrating.
7. Get additional information and support, as needed.

Establish functional teams

Gather your most skilled people and establish the following functional teams:

- Directory services (CED, Exchange, master user domains)
- Administration and management (tools, processes)
- Core OS (print, file systems, domains, performance)
- Networking (DNS, WINS, Dynamic DNS, protocols, bandwidth)
- Workstation (install/upgrade, inter-operability, configuration, applications)
- Hardware compatibility
- Architecture (the rollup)

Have your teams evaluate Windows 2000 press releases and customer advisories, examine your current system, and plan and design your Windows 2000 test environment. Plan on several months to correctly plan your upgrade strategy.

Understanding the structure and function of Active Directory

Active Directory is the core of each Windows 2000 system and provides a consistent way to name, describe, locate, access, manage, and secure information about resources throughout an enterprise. It then makes this information available to users.

> **NOTE:** Active Directory is a fully extensible and scalable network service that provides a single point of administration for all published resources

This network of infrastructure services extends the features of previous Windows-based directory services and works well in installations of any size, from a single server with hundreds of objects to thousands of servers and millions of objects.

More specifically, Table 1 outlines how Active Directory can meet your specific business needs.

Table 1. How Active Directory meets your business needs

Business needs	Active Directory solution
Reduced TCO	Group Policy within Active Directory allows you to configure desktop environments and install applications from an administrative console. This reduces the time normally needed to visit each computer independently to configure settings and install applications.
Simplified administration	Active Directory provides a single location to store information about users and resources. This simplifies administration and makes it easier for users to find resources throughout a network.
Flexible administration	Active Directory increases administrative flexibility by allowing you to delegate the authority of users and computers to other users or groups, such as administrators. This allows you to specify the users who will have administrative authority over portions of your network.
Scalability	In Windows NT 4.0, domains have a practical limit of 40,000 objects. Therefore, you must create many domains for a large organization. In Windows 2000 Server, an Active Directory domain can contain millions of objects.
Standards-based protocol	Access to Active Directory is achieved through the Lightweight Directory Access Protocol (LDAP) protocol. Applications can use LDAP rather than proprietary protocols to access and change information in Active Directory.

The goal of Active Directory is to provide a unified view of the network that will greatly reduce the number of directories and namespaces with which network administrators and users must contend. Active Directory is specifically designed to inter-operate with other directories, regardless of their location or their underlying operating systems. To accomplish this, Active Directory provides extensive support for existing Internet standards and protocols. It provides application-programming interfaces (APIs) that facilitate communication with these other directories.

Table 2 describes the technologies that Active Directory supports, the purpose of the technology, and a reference for more information on the technology.

Table 2. Technologies that Active Directory supports

Technology	Purpose	Reference
Dynamic DNS	Host namespace management	RFC 2052 and 2163
Dynamic Host Configuration Protocol (DHCP)	Network address management	RFC 2131
Kerberos version 5	Authentication	RFC 1510
LDAP v3	Directory access	RFC 2251
LDAP'C'	Directory API for programming	RFC 1823
LDAP Data Interchange Format (LDIF)	Directory synchronization	Internet Engineering Task Force (IETF) Draft
Simple Network Time Protocol (SNTP)	Distributed time service	RFC 1769
TCP/IP	Network transport	RFC 791 and 793
X.509 v3 certificates	Authentication	International Organization for Standardization (ISO) X.509

Supporting these Internet standards provides several benefits:

- DNS dynamic update protocol enables corporations to achieve a global naming structure that is compatible with standard Internet DNS conventions.
- LDAP maximizes the interoperability between applications and directory services and facilitates directory inter-operability through synchronization.
- Kerberos v5 and X.509 certificate integration with Active Directory gives corporations the flexibility to mix and match the security that they deploy—in both Internet and intranet environments—based on their needs.

The logical and physical structure of the Active Directory

To administer or support a Windows 2000 network, you must understand the functionality and structure of Active Directory. In the Active Directory, the logical structure is separate from the physical structure. See Figure 1.

You use the logical structure to organize your network resources, and you use the physical structure to configure and manage your network traffic.

The logical (functional) and physical structure of Active Directory have no correlation

Logical Structure
(organize network
resources)

Physical Structure
(configure and manage
network traffic)
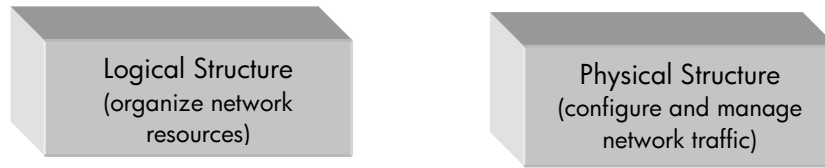
The logical structure of Active Directory

The logical structure of Active Directory is flexible and provides a method for designing a directory hierarchy that makes sense both to users and to those who manage it. A typical directory structure includes forest, trees, domains, organizational units, and objects.

At the bottom of the hierarchy are objects that represent network resources, such as user objects, computer objects, and printer objects. See Figure 2. In Windows 2000 you can give control at the object level; in Windows NT, you could only give control at the domain level. This greatly reduces the number of domains that you must create and manage.

Figure 2. Active Directory objects are network resources, such as users, computers, and printers
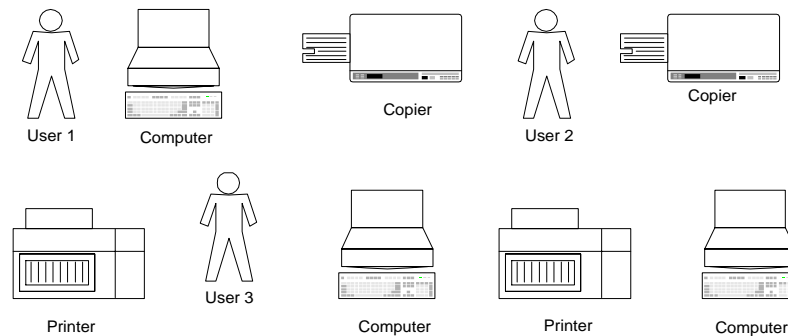

Whenever you add new resources to your network, you create objects that represent these resources, and then manage the access to them.

You can organize objects within a domain into containers, which are called organizational units (OUs). Organizational units can also be grouped into other OUs. Employing OUs to contain and organize the objects in Active Directory is similar to using folders to contain and organize other folders and files.

Referring to Figure 3, you can see similar objects have been grouped according to administrative responsibilities, or in simpler terms, the objects are grouped into containers that different managers— such as the printer administrator or the user administrator—can control. The section "More About Organizational Units" will describe another way to group objects.

Figure 3. Organizational units within a domain


OU-Printers OU-Users OU-Computer
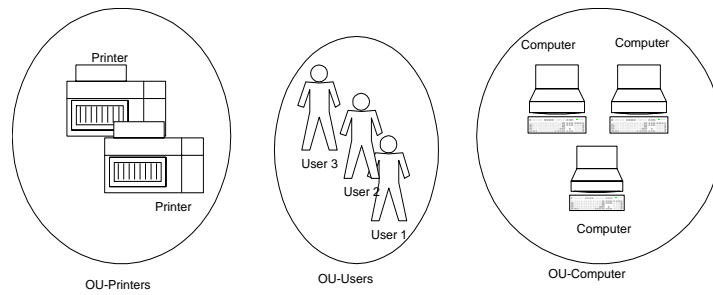
The core unit of the logical structure in Active Directory is the domain. A domain is a logical grouping of servers and other network resources (grouped into OUs) that share a common directory database defined by an administrator. In Figure 4, all the objects grouped into one domain have access to the same directory database. In Figure 5, every domain also has its own security policies and security relationships (trusts) with other domains. Also see the section "Trust Relationships."

Figure 4. Active Directory domains are logical groupings of objects and OUs that have access to the same database
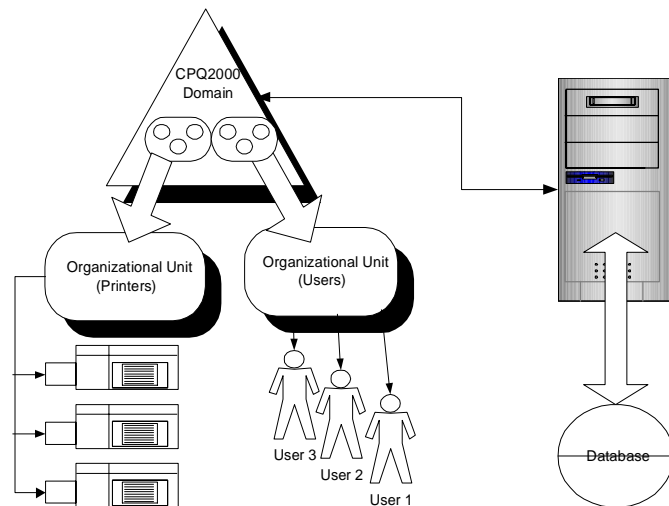
The last two logical structures of the Active Directory are trees and forests. A *tree* is a group of one or more domains, all of which share a contiguous DNS namespace, while a *forest* is a collection of two or more trees that form a noncontiguous DNS namespace. See Figure 5.

10

Figure 5. The logical structure of Active Directory
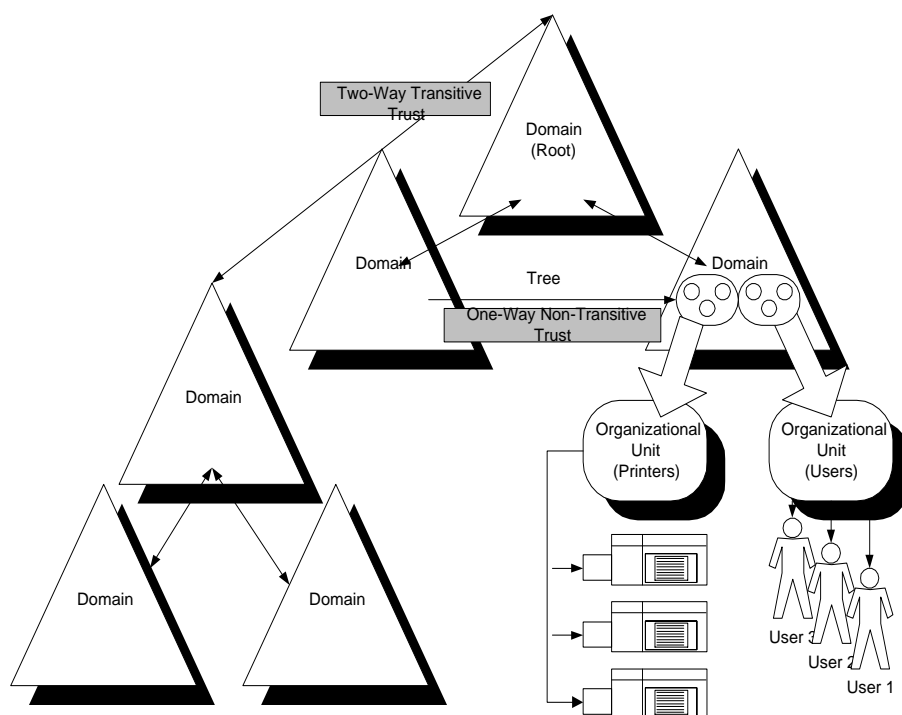
Remember to allocate sufficient time for establishing domains, and the OUs and objects within each domain, when you plan your Windows 2000 upgrade. The performance and efficiency of your network operations will depend upon the way you design the logical and physical structure of your directory.

The next sections cover each part of the logical structure in more detail to help with your Active Directory design.

More about objects

To locate network resources, your users and applications must know the name or some property (attribute) of the resource object. Active Directory supports many naming conventions that allow users and applications to use the format with which they are most familiar.

Every object in Active Directory must have a distinguished name that identifies the domain where the object is located, in addition to the complete path by which you can reach the object. The relative distinguished name is the part of the distinguished name that is an attribute of the object.

Windows 2000 also assigns a globally unique identifier (GUID) to objects when they are created. Applications can store the GUID of an object and be able to retrieve that object even if the distinguished name changes.

Every object in the Active Directory also has a security descriptor that defines (1) who has permission to access the object, and (2) the specific actions that each user can perform on the object. To reduce administrative overhead, you can group objects with identical security requirements into one OU. You can then grant permissions to the entire OU and, consequently, to all objects within it. Windows 2000 then stores these user access permissions in the DACL, a discretionary access control list.

Groups simplify administration by allowing you to grant permissions once to a group rather than multiple times to individual users. Two group types are security groups and distribution groups.

Use security groups to grant or deny rights and permissions to groups of users and computers; use distribution groups for sending emails with applications such as Microsoft Exchange Server. During the logon process, Windows 2000 creates an access token that contains the list of security groups to which the user belongs. Using distribution groups instead of security groups improves logon performance by reducing the size of access tokens.

Both groups have a scope attribute that determines who can be a member of the group and where you can use that group in the network. There are three attribute types:
(1) domain local, (2) global, and (3) universal.

Domain local groups contain user accounts, global groups, and universal groups from any domain in the forest, as well as local domain groups from the same domain. You can only grant permissions to domain local groups for objects within the domain in which the domain local group exists.

Global groups contain user accounts and global groups from the domain in which the group exists. You can grant permissions to global groups for all domains in the forest, regardless of the location of the global group.

Universal groups contain user accounts, global groups, and other universal groups from any Windows 2000 domain in the forest. You can grant permissions to universal groups for all domains in the forest, regardless of the location of the universal group.

NOTE: The object type determines which permissions you can select. Permissions vary for different object types. For example, you can grant the Reset Password permission for a user object, but not for a printer object.

A user can also be a member of multiple groups, each with different permissions that provide different levels of access to objects. When you grant permission to a user for access to an object, and that user is a member of a group to which you granted a different permission, the user's effective permissions are the combination of the user and the group permissions. For example, if a user has the Read permission and is a member of a group with the Write permission, the user's effective permission is Read and Write.

More about organizational units

OUs are Active Directory containers—groupings of objects, such as user accounts, groups, and computer accounts—within a domain. Because OUs can contain other OUs, you can extend a hierarchy of containers to model your company organizational structure or administrative needs. You can then delegate administrative control by granting specific permissions for OUs—and the objects that they contain—to other individuals and groups. You have a wide range of permissions that you can grant. You can assign complete administrative control (for example, full control over all objects in the OU) or limited administrative control (for example, the ability to modify email information on user objects in the OU).

NOTE: You must have Read, List Contents, and Create Organizational Unit Objects permissions on the parent container (domain or OU) to create OUs within that container. (List Contents is not absolutely required, but you cannot view the newly created OU without it.) By default, members of the Administrators group have the permissions to create OUs anywhere.

Administrators group have the permissions to create OUs anywhere.

You can employ OUs to group objects into different logical hierarchies that represents one of two operating mindsets:

- Your company's network administrative model. For example, at your company, there might be one administrator who is responsible for all user accounts and a different administrator who is responsible for all printers. In this case, you would create an OU for users and a different OU for printers. Refer back to Figure 3.
- Your company organizational structure, based on department or geographical boundaries. For example, if your company has divisions in Houston and Paris you can create a separate OU for each location, allowing you to manage and delegate control of each division easily.

Figure 6 illustrates how the same objects can be grouped differently.

Figure 6. Different methods of establishing OUs
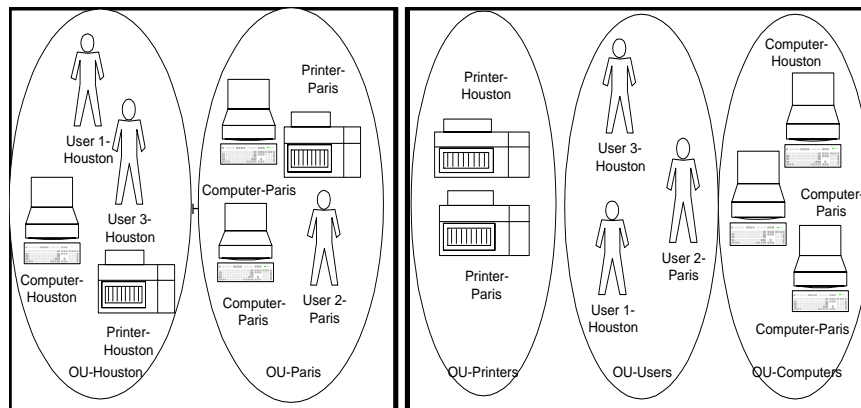
To create OUs based on your organizational structure, your OUs might look like the groupings in the left-hand box in Figure 6. You will only have two OUs that mirror your organizational structure and control: a Houston-based operation and a Paris-based operation.

To create OUs based on your network administration, see the right-hand box in Figure 6. You will have three OUs: printers, users, and computers.

> **NOTE:** The OU hierarchy within a domain is independent of the OU hierarchy structure of other domains. That means you can implement a network administrative OU hierarchy in one domain and a company organizational structure in another domain..

Domains

In a Windows 2000 network, the domain serves as a security boundary. The administrator of a domain has the necessary permissions and rights to perform administration within that domain only, unless you explicitly grant your administrator those rights in another domain.

The first Windows 2000 domain created is the root domain, which contains the configuration and schema for the forest. Additional domains are added to the root domain to form the tree structure or the forest structure, depending on the domain name requirements.

- Single versus multiple domains

  As a rule of thumb, start with a single domain and prove that you need more. HP has business units in many states and foreign countries (161) yet the company uses only three domains (and a top-level placeholder domain) to manage the HP infrastructure. Everything else is based around OUs.

Other important factors to consider are replication factors, group policy, administrative boundaries, and hardware considerations. These factors are discussed in the section "Planning, preparing, and designing tipsheet."

- Domain naming

Domain structure and naming evolves around the Internet. The root domain is at the top of the domain structure and is represented by a period. Below the root, top-level domains can be represented by organizational type, such as .com or .edu, or represented by geographical location, such as .au for Australia. Second-level domains are registered to individuals or corporations. When you add a domain to an existing tree, the new domain is a child domain of an existing parent domain. The name of the child domain is combined with the name of the parent domain to form its DNS name.

Also see the section "Domain name service (DNS)."

Forests and trees

Recall that a forest is a collection of two or more trees that form a noncontiguous DNS namespace. It is useful in organizations that need to maintain separate organizational structures, such as a company that needs distinct public identities for its subsidiaries. Every Active Directory forest must have domain controllers that fulfill each of the five operations master roles. See the section "Domain controllers."

Recall that a tree is a group of one or more domains, all of which share a contiguous DNS namespace.

Trees in a forest share three things:

- Transitive trusts
- Common schema
- Common global catalog

Each tree in a forest has its own unique namespace. Although two companies do not share a common namespace, by adding a new Active Directory domain as a new tree in an existing forest, two companies could share resources and administrative functions.

Trust relationships

Active Directory supports two forms of trust relationships: one-way, non-transitive trusts and two-way, transitive trusts. Look back at Figure 5.

- One-way, non-transitive trusts

In a one-way trust relationship, domain A trusts domain B, but domain B does not automatically trust domain A. In a non-transitive trust relationship, if domain A trusts domain B and domain B trusts domain C, domain A does not automatically trust domain C.

Windows NT networks use one-way, non-transitive trust relationships. Since you have to manually create one-way, non-transitive trust relationships between existing domains, this type of trust—in a large network— imposes a large amount of administrative overhead.

Active Directory supports one-way, non-transitive trusts for connections to Windows NT networks. You can also establish one-way, non-transitive trusts between Active Directory domains. For example, if you want to allow an external business partner to have access to resources in a particular domain while working on a joint project, you might create a one-way, non-transitive trust between the internal and external domains.

- Two-way, transitive trusts

In a two-way trust relationship, if domain A trusts domain B, then domain B automatically trusts domain A. In a two-way transitive trust relationship, if domain B trusts domain A and domain C

trusts domain A, then domain B automatically trusts domain C and domain C automatically trusts domain B.

If a two-way, transitive trust exists between two domains, you can grant permissions to resources in one domain to user and group accounts in the other domain, and vice versa. Two-way, transitive trust relationships are the default between Windows 2000 domains.

The physical structure of Active Directory

The physical structure of Active Directory defines where and when replication and logon traffic occur. Understanding the physical components of Active Directory is critical to optimizing network traffic and the logon process. In addition, this information can help in troubleshooting replication and logon functions.

> **NOTE:** There is no necessary correlation between site and domain name spaces.

The physical structure of Active Directory is composed of sites and domain controllers. A site is a combination of one or more IP subnets that are connected by a high-speed link. See Figure 7. Active Directory makes the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where the resource is or how it is physically connected, such as in the case of a printer.

Figure 7. The physical structure of your Active Directory includes sites and subnets
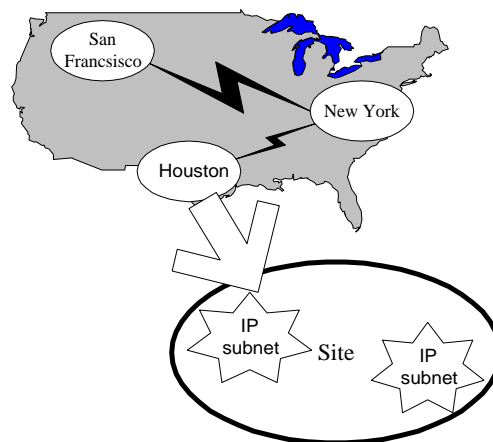
Sites

Sites are beneficial in organizations that have geographically separated locations that are connected by slow links. Sites help reduce Active Directory traffic, such as workstation login traffic and replication traffic, and enable users to connect to a domain controller by using a reliable, high-speed connection. At HP, a site is defined as a 512-KB link with 256 KB of excess capacity.

When designing your physical site structure to optimize your logical structure, keep these points in mind:

- Sites are physically discrete locations in your network.
- Sites are, by definition, areas of high connectivity.
- Site links define connectivity between sites. The placement and location of site links tell Active Directory how and where to replicate information in your network.
- Base your inter-site replication upon your current WAN topology and available bandwidth.

- Move domain controllers into their respective sites to establish the replication topology for your network.
- Active Directory allows multiple domains in a single site, as well as multiple sites in a single domain.
- After configuration of a site, you can edit the site link properties to configure cost, replication intervals, and replication schedules to optimize replication traffic across the site link.

> ✓ **IMPORTANT:** Sites map the physical structure of your network, whereas domains map the logical structure of your organization.

Domain controllers

A domain controller is a computer running Windows 2000 Server that stores a replica of the directory. It manages user logon processes, authentication, and directory searches. It also manages the changes to directory information and replicates those changes to other domain controllers within the same domain.

> **NOTE:** Domain controllers might hold different information for short periods of time until all of the domain controllers have synchronized their changes to Active Directory.

In Windows 2000 networks, Active Directory uses multi-master replication, in which no single domain controller is the master domain controller. All domain controllers running Windows 2000 have equal status in the domain. When you upgrade primary domain controllers (PDC) and backup domain controllers (BCD)—running Windows NT 3.51 or Windows NT 4.0—to Windows 2000, there is no longer a distinction between them. In Windows NT 4.0, the PDC contains the only writeable copy of the domain database; but in Windows 2000, all domain controllers contain a writeable copy of the directory database. So they could be called peer domain controllers.

A domain can have one or more domain controllers. A small organization using a single local area network (LAN) might need only one domain with two domain controllers to provide adequate availability and fault tolerance. A large company with many geographical locations might need one or more domain controllers in each location to provide adequate availability and fault tolerance.

To log on to the network and perform queries in Active Directory, a computer running Windows 2000 must first locate a domain controller or a global catalog server, to process the logon authentication or the query. The DNS database stores the information about which computers perform these roles and provides that information so that the request can be directed appropriately.

Although Active Directory supports multi-master updates of the directory between all of the domain controllers in a domain, some changes are impractical to perform in multi-master fashion because of replication traffic and the potential for conflicts in essential operations. For these reasons, special roles, such as global catalog server and operations masters, are assigned only to specific domain controllers. An understanding of these roles is important because if a domain controller that holds these roles is not available, the specific functions of that role in Active Directory will not be available.

Global catalog server

The global catalog is a repository of information that contains a subset of attributes for all objects in Active Directory. By default, the attributes that are stored in the global catalog are those that are most frequently used in queries (such as a user's first name, last name, and logon name). The global catalog contains the information that is necessary to determine the location of any object in the directory.

A global catalog server is a domain controller that stores a copy of and processes queries to the global catalog. Global catalog servers improve the performance of forest-wide searches in Active Directory. For example, if you search for all of the printers in a forest, a global catalog server

processes the query against the global catalog and then quickly returns the results. Without a global catalog server, this query would require a search of every domain in the forest.

> **NOTE:** If a user is a member of the domain admins group, then the user can log on to the network even when the global catalog server is not available.

When a user logs on to the network, the global catalog server provides universal group membership information for the account to the domain controller that processes the user logon information. Look at Figure 8. If a global catalog server is not available when a user initiates a network logon process, then the user is only able to log on to the local computer.

The first domain controller that you create in Active Directory will be a global catalog server. You can also configure additional domain controllers to be global catalog servers in order to balance the logon authentication traffic and query traffic.

Figure 8. The global catalog server responds to objects anywhere in the domain or forest
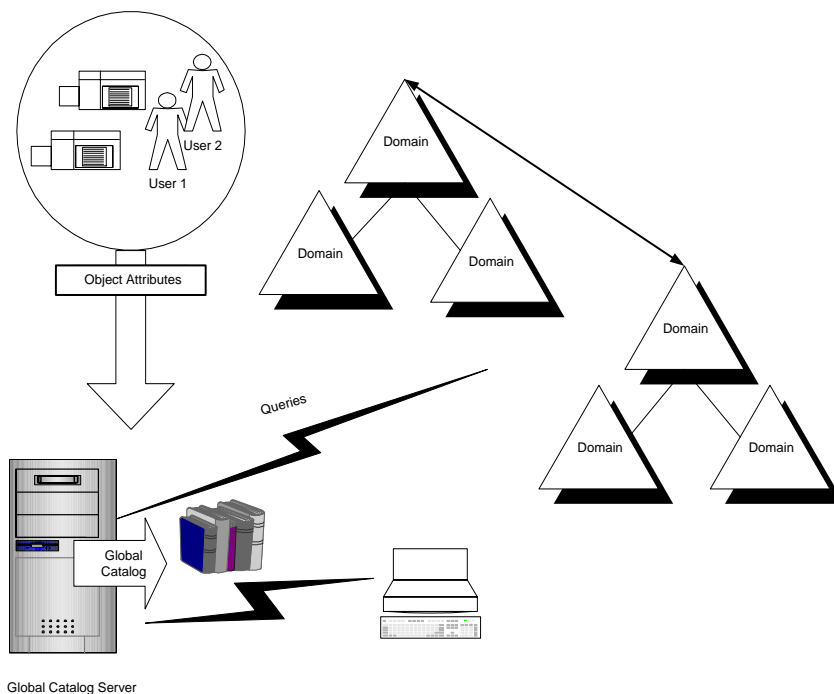
The global catalog server is designed to respond to queries about objects anywhere in the domain, tree, or forest with maximum speed and minimum network traffic. Because a single domain global catalog server contains information about objects in all domains in the forest, a global catalog server––in the domain in which the query is initiated—can resolve a query about an object. So, finding information in the directory does not produce unnecessary traffic across domains.

Operations master server

An operations master is a domain controller assigned one or more special roles in an Active Directory domain. The domain controllers assigned to these roles perform single-master operations, or operations not permitted to occur at different places in the network simultaneously.

- The domain controller that controls a particular operation owns the operations master role for that operation. The ownership of these operations master roles can be transferred to other domain controllers.

✓ **IMPORTANT:** Only one domain controller can own an operations master role at any one time.

- Every Active Directory forest must have domain controllers that fulfill each of the five operations master roles.
- Schema master controls all updates and modifications to the schema.
- Domain naming master controls the addition or removal of domains in the forest.
- Relative identifier (RID) master allocates sequences of RIDs to each of the various domain controllers in its domain.
- Primary domain controller (PDC) emulator receives preferential replication of password changes that are performed by other domain controllers in the domain.
- Infrastructure master updates the group-to-user references whenever group memberships are changed. Each domain in the forest must have one infrastructure master.

Domain modes

After you install Active Directory and establish a domain, the domain and Active Directory are running in mixed mode. A mixed-mode domain supports domain controllers that are running either Windows 2000 or Windows NT. Active Directory installs in mixed mode to provide support for existing domain controllers that have not been upgraded to Windows 2000. You can operate your domain in mixed mode indefinitely, which allows you to upgrade domain controllers running Windows NT on a schedule that meets the needs of your organization. When all domain controllers have migrated to Windows 2000, you will be running in native mode.

User accounts

User accounts, employed to authenticate users, also grant specific permissions to gain access to network resources. You can use Active Directory users and computers on any available domain controller to create a new user account. After you create the account, it is replicated to all of the other domain controllers in the domain.

When you create the user account, you must first select the OU in which to create it. You can create accounts at the domain level, but doing so limits your delegation options and increases the complexity of managing your network.

Username (user principal name) is the user's complete name and the DNS name of the domain where the user object resides, which Active Directory displays as the user account name. First name and last name are attributes of the user account that might be used in search operations to locate the user account. The value that you assign to these two attributes does not need to be unique at any level in the forest; however, it must be unique within the container where you create the user accounts.

After you have established usernames for your user accounts, you can set the password requirements and options shown in Table 3.

Table 3. Password requirements and options

Option	Description
Password	Used to authenticate the user. **Tip**: Always assign a password.
Confirm password	Typing the password a second time to ensure you entered it correctly.
Change password at next logon	Making a user change his or her password the first time he logs in to ensure that the user is the only person who knows the login.
Cannot change password	Allows only administrators to control password. **Tip**: Works

Option	Description
	extremely well if you have more than one person who uses the same domain user account.
Password never expires	Self-explanatory.
Account disabled	Prevents use of this account. **Tip**: Use this option to set up an account for a new hire who has not yet started.

Domain name service (DNS)

Domain Name Service (DNS) is a database that Microsoft Windows 2000 uses as its primary method for name resolution and service location. DNS is used in TCP/IP networks to translate computer names into IP addresses and to locate domain controllers that provide user authentication. In Windows 2000 DNS can use hierarchical fully qualified domain names (FQDNs), instead of the NetBIOS naming conventions that Windows Internet Naming Service (WINS) supports. This is a great advantage since the FQDN describes the exact location of a host to its domain.

> **NOTE:** Microsoft Windows will continue to support WINS.

An integral part of client/server communications, DNS consists of (1) a tree of uniquely-named domains, (2) servers that contain information about some segment of that tree (name servers), and (3) clients who query DNS to get IP addresses resolved to computer names (resolvers).

> **NOTE:** If your Active Directory plan includes using your DNS name externally, for example, on the Internet, you must choose a unique domain name and register it with the Internet Network Information Center (InterNIC) to assure that it is unique on the Internet.

The Windows 2000 implementation of DNS includes several new features that improve upon the DNS capabilities provided in Windows NT 4.0 and that ease the administrative burden of maintaining the database. These features include the new SRV (service resource records). These resource records are particularly helpful by enabling you to identify network resources. (These records actually perform the same task as the sixteenth character of a NetBIOS name that is stored in a WINS database.)

In addition, Windows 2000 DNS features include incremental zone transfer and integration with Active Directory, as well as configuration wizards and other tools to help you manage and support DNS name servers and clients on your network.

Client computers can query a DNS name server to obtain IP addresses for computers that host a particular service. For example, if a client computer must find a computer that will validate logon requests, the client computer can send a query to a DNS name server to obtain a list of domain controllers and their associated IP addresses. And since the implementation of Windows 2000 DNS supports dynamic update protocol, client computers can automatically update DNS name servers so that resource records can be updated without administrator intervention.

As you can see, there is much to consider when designing your logical and physical network structure. You need plenty of time to carefully plan your Windows 2000 environment.

Examine your current system

We have all heard the old cliché "Learn from the past." Well, that advice should be heeded before designing your new Windows 2000 environment. By making your commitment to Windows 2000 early, you can take the opportunity to fully understand your current environment and fix any Windows NT 4.0 problems before designing your new system.

At a minimum, do the following:

- Understand where your resource domains are and why they are there.
- Examine your master user domains (MUDs). How many do you really need?
- Determine where the centers of administration are located.
- Determine if the current LAN/WAN topology can sustain your company's future needs.
- Make sure your current platforms are up-to-date and standardized.
- Determine what software and hardware tools you have and what you will need.
- Ensure that all applications and services currently residing on your server will run with Windows 2000.

At this point you should clearly understand the differences between your current network (topology) and a Windows 2000 network. Table 4 is a quick reference chart comparing some Windows NT and Windows 2000 Active Directory terms and usage.

Table 4. Comparison of Windows NT topology with Windows 2000 topology

Item	Windows NT	Windows 2000
Control	Attached to domains	Can be given to objects
Domain	Geophysical grouping	Logical grouping
	Smallest administrative boundary	See User (object).
Masters	Single master for updates per domain	Multiple Master Model, plus cross-domain
Mixed steppings	Mixed steppings supported	Some mixed processor configurations can cause the system to hang during installation. Visit this website for more information: http://h18000.www1.hp.com/products/servers/processor-mixing/.
Replication	Can easily get out of control	Can be controlled
Trust Relationship	Complicated	Transitive, not exponential
User (object)	Limit of <40000	10 to 20 million
		Smallest administrative boundary

Prepare your current system for Windows 2000

Before you decide on an upgrade strategy, take the time to cleanup your current system. It will save some time when you actually design and pilot your new system. Besides, you will gain a better understanding of your network infrastructure.

- Clean up your master user domain namespaces and resolve duplicate names across the enterprise.
- Resolve duplicate usernames across the enterprise, especially if you have had recent mergers and acquisitions.
- Clean up Windows Internet Naming Service (WINS) and make sure that it works properly.

WINS is the service that Microsoft Windows uses in addition to Domain Naming Service (DNS) to be able to match computer addresses with names. Under Windows NT, it is a dynamic service: servers

and clients automatically register themselves with this service, and it is the way to know how to find a machine.

- Consolidate your DNS architecture and administration.
- Collapse unneeded resource domains.
- Decide what you will do with your (remaining) resource domains.
- Ensure that the latest Service Packs are loaded.
- Audit your security environment.
- Buy desktops and portables that meet Microsoft Windows 2000 Ready PC requirements. See www.microsoft.com/whdc/hcl/default.mspx. All currently shipping HP Desktop and Notebook products meet the Ready PC requirements.
- Ensure that all third-party products are compatible with Windows 2000.
- Upgrade your servers and options to capitalize on the performance and scalability of Windows 2000. (HP continues to work with Microsoft Windows Hardware Quality Lab to ensure complete compatibility of Windows 2000 with all supported HP products.) Check the Windows Hardware Compatibility List website at www.microsoft.com/whdc/hcl/default.mspx to ensure hardware compatibility.

Planning, preparing, and designing tipsheet

Although this Integration Note does not cover the explicit details of designing your Active Directory or preparing a comprehensive upgrade plan, we have gathered some of our best tips from personal experiences and pass them to you:

- You must review and prepare the existing Windows NT infrastructure before you can plan and design your Windows 2000 infrastructure.
- You can create your infrastructure with fewer machines, but correct setup is much more critical.
- Windows NT 4.0 servers can co-exist within the same domain as a Windows 2000 server.
- You should aggressively (proactively) migrate all clients, particularly mobile clients, to Windows 2000; Professional Workstations, DeskPros, and Armada PCs should be purchased with Windows 2000 pre-installed.
- Having many subsidiaries usually equates to having many sites.
- Primary factors to consider when planning single versus multiple domains:
  - Replication — In using a single domain, you give up a lot of control, but you can still schedule connection object replication. There are no site links, no site link bridges, no least-cost-path, and so forth. If you have good connectivity (relative term), then maybe this is not that much a concern. Remember that in a single domain, all domain controllers are essentially global catalog servers; therefore, you will probably have more replication traffic in a single domain, but information will be faster to access.
  - Group policy — A single domain eliminates the need for universal groups, global groups, and so forth, making administration simpler. However, some policies are domain level only. Plan your policies to see which group policy applies to which group of users. Sharing policy across domains is not as efficient as intra-domain sharing of policies.
  - Decentralized network administration — If your political organization allows everyone to be controlled by one group, then a single domain might be the way to go. However, your company might have separate, autonomous business units, almost like separate companies. They may even have separate information technology groups and separate CEOs. In this case, you may need a separate domain for each business unit. However, administrative overhead increases as domains increase: more hardware (see next bullet), more backups, more supplies, and so forth.
- Hardware — Every domain requires a lot of hardware. At a bare minimum, you will need three domain controllers per domain: one PDC and two replicas just to be safe (one non-global catalog

can be the infrastructure master). On the other hand, if you use more OUs, there are no additional domain controllers to install, promote, maintain, and so forth.

- Other reasons to create more than one domain
  - Different password requirements between organizations
  - Large number of objects
  - Different Internet domain names
  - Multinational organizations that require local administration to be performed in different languages

- Determine the number of domain levels based on your Active Directory structure. Every Active Directory domain must have a corresponding DNS domain. If you have an existing DNS namespace, it should not determine your Active Directory structure. Rather, DNS should accommodate Active Directory. It is possible, however, to keep your existing DNS namespace and create a new one for Active Directory.

- An effective naming strategy is important to help your organization take advantage of Windows 2000 functionality. An effective naming strategy also makes it easier for users to log on to the network and to locate network resources.

- Avoid lengthy domain names
  - Domain names can be up to 63 characters, including periods.
  - The total length cannot exceed 255 characters. This is especially important if you have many levels of domains because you might potentially exceed naming limitations.

- Fully qualified domain names can become too lengthy if domain names are very long.
- WINS will be necessary until none of your applications require NetBIOS.
- Establish and tune replication between domains, trees, and forests.
- Design inter-domain replication for global catalog.
- Use global groups wherever possible to help with your migration or upgrade.
- Investigate opportunities to consolidate company directories. Migrate and populate user data from existing systems to Active Directory.
  - Human Resource systems
  - Microsoft Exchange mail and messaging system.
  - Meta-directories

Application services are the second component. These are the primary business applications that organizations deploy to fulfill business requirements or to improve user efficiency and communications.

- Most resource domains will migrate to OUs.

And we saved the best tip for last: Improve your time to success by partnering with HP, the most experienced service company.

Piloting and validating your Windows 2000 environment

Pilot and validate means to set up a test environment that will mirror your final system. Start your evaluation and pilots to get some real life experience, work the kinks out of your upgrade strategy, and make your mistakes BEFORE you start migrating.

Unlike previous versions of Windows NT, the migration to Windows 2000 can and will extend over a very long time, perhaps as long as two to three years until you have finished migrating all resource domains.

Once you decide where you are, how you got there, and what is available, determine where you want to be and how to get there. What security issues are most important? How long can you allow

for full migration? Develop an upgrade roadmap with clearly defined action programs to make sure you have a strategy that can work.

> ✓ **IMPORTANT:** You should understand the supported upgrade paths for Microsoft Windows 2000: Windows NT 3.51 and Windows NT 4.0 can upgrade to Windows 2000 Server Edition; Windows NT Enterprise can upgrade to Windows 2000 Advanced Server Edition. Attempts to upgrade Windows NT 3.51 or Windows NT 4.0 to Windows 2000 Advanced Server Edition will result in a dual-booting system, and your data will not transfer to Windows 2000.

Also be aware of these items:

- Clients need to be Active Directory aware.
- Windows NT 4.0 workstations will easily migrate to Windows 2000 Professional.
- Windows 9X workstations need the Active Directory Client Upgrade package.
- Down-level clients will still operate as if in a Windows NT domain.
- You cannot move to native mode until your entire infrastructure is Windows 2000.
- Microsoft Exchange 2000 shares the same Active Directory as Windows 2000 but retains a separate database. You will be able to access email messages, web pages, applications, and even streaming video and audio content from Outlook, as well as from a wide range of other client software.

Also look at the white papers *Implementing Microsoft Windows 2000 with Service Pack 4 on ProLiant servers* and *Upgrading to Microsoft Windows 2000 on ProLiant servers* on the HP ISS Technology Papers website at www.hp.com/servers/technology website. With these things in mind, you have two basic strategies: migration or restructuring. However, in reality, most upgrades will include a hybrid of these two. Here are some major points to consider.

Migration strategy

- If you feel comfortable with your current domain structure and want to basically keep things as they are, you might just want to migrate your current system structure to your new Active Directory. Here are some things to think about.
- All your access controls, security, and so forth will remain the same.
- Your existing hardware, however, might not support Windows 2000.
- Once you start, you are committed and will have to migrate an entire domain at once. Who will migrate first? How will you determine when the next group is ready to migrate?
- Any pilot environment will be a throwaway.

Restructuring (build new) strategy

This upgrade strategy allows you to start from scratch and build a new directory service. Keep these things in mind:

- You have the opportunity to improve your domain structure.
- You still have to migrate access controls and security (few tools exist to do this).
- You can build new infrastructure on hardware that has a future.
- Your upgrade can be more methodical, and you will always have a back out.
- Your pilot becomes the core of your rollout.

> **NOTE:** Regardless of the method you choose, domain trust issues will be problematic the longer you take to reach full implementation.

A word of advice: The deployment of Windows 2000 to the enterprise is not a simple task. Do not roll it out until you have thoroughly tested it.

Additional information and support

Now that you understand Microsoft Windows 2000—its benefits, complexities, and opportunities—and have heard all about developing an efficient Active Directory and starting your pilot program, you might still have some confusion about upgrading.

HP support for Windows 2000

HP Services, Microsoft's chosen deployment partner and premier platform provider, provides both equipment (from portables to servers) and staff at all the deployment events (see the next section) and in the test labs on the Microsoft campus.

Primary consulting and education activities include the following:

- Assisting in architecture and development
- Planning domain and network resource consolidation
- Creating test plans for directory integration and migration strategies
- Ensuring complete inter-operability and compatibility
- Reducing TCO

HP Services also helps you follow best practices and gives you a better understanding of how Windows 2000 will operate in your future framework. The HP On Track for Windows 2000 Services offers customer assistance through all the phases of migrating to Windows 2000. Key items covered in the program include the following:

- Assessment for Windows 2000
- Planning and designing for Windows 2000
- Design reviews for Windows 2000 implementation
- Pilot for Windows 2000
- Support and management

HP Services also provides application integration to help understand how to integrate UNIX/Microsoft Windows NT, the Internet, and enterprise applications. The typical Architecture Service is a five-day engagement that is deliverable focused. Senior HP Solutions Architects staff the Services lab where you (and 2 to 7 more customer developers) can get actual hands-on experience.

To learn more about HP Services, visit the website at www.hp.com/hps/.

HP support software and documentation

HP is the best solution for deploying Windows 2000. HP products deliver the following:

- Easy software deployment or upgrade to Windows 2000
- Unmatched compatibility with Windows 2000 and related applications
- Optimized performance for Windows 2000
- Industry leading manageability for Windows 2000

For Windows 2000, HP provides and distributes support utilities, drivers, and other information on the SmartStart CD, Management CD, and a myriad of websites.

HP websites are brimming with helpful information. Start with the Frontline Partnership website www.hp.com/go/microsoft.

Microsoft support for Windows 2000

Microsoft initiated the Deployment Program for Windows 2000 to create awareness and gain practical feedback from customers on the deployment of Windows 2000 before actual release.

You can learn more about migration programs on the Microsoft website at www.microsoft.com/windows2000/techinfo/planning/default.asp or the HP website at www.hp.com/hps/.

Deployment conferences

As part of the deployment, Microsoft sponsored Deployment Conferences that were powered exclusively by HP. These conferences and labs enabled early adopters to plan the architecture of their Windows 2000 Professional and Server deployment. The conferences also helped adopters develop effective strategies for migrating from their current operating system environment and integrating Windows 2000 with their existing network infrastructure.

Microsoft websites

Microsoft also has a wealth of migration tools and information available to customers on its websites. Table 5 lists the most popular and helpful sites. Since information funnels into the site almost daily, keep checking for the latest information.

Table 5. Microsoft websites for Windows 2000 information and products

Item	Web location
Business Customer Support	www.microsoft.com/support/customer/enterprise.htm
FAQs	www.microsoft.com/ntserver/support/faqs.asp
Internet Support Options	www.microsoft.com/ntserver/support/
Security Issues	www.microsoft.com/security/default.asp
Technology Issues	www.microsoft.com/technet/
Windows 2000 Server	www.microsoft.com/windows2000/
Windows 2000 Newsgroups	www.microsoft.com/ntserver/support/newsgroups/Win2000.asp
Windows NT Knowledge Base	http://support.microsoft.com/
Windows NT Newsgroups	www.microsoft.com/ntserver/support/newsgroups.asp
Windows NT Workstation	www.microsoft.com/ntworkstation/default.asp
Windows NT Server	www.microsoft.com/ntserver/

Conclusion

Start now to plan and prepare for Windows 2000. And, remember to plan your hardware upgrades to take advantage of new levels of processors and memory available with Windows 2000. By starting your evaluation and pilots early, you will get some real-life experience and make your mistakes before you try to upgrade your entire network. Most importantly, partner with HP.

Windows 2000 and its directory services will make your environment more efficient, and productive, and it will reduce TCO. You cannot afford to miss the advantage!

For more information

Visit the HP Windows 2000 website at www.hp.com/go/microsoft for the latest information about HP products, options, customer support, and documentation regarding Microsoft Windows 2000 products.

Call to action

To help us better understand and meet your needs for ISS technology information, please send comments about this paper to: TechCom@HP.com.

TC030614IN, 6/2003